207 - Trattamento per whistleblowing

Numero identificativo:	**207**
Finalità	Trattamenti dei dati personali delle persone fisiche per la gestione delle segnalazioni di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.
Condizioni di liceità del trattamento (base giuridica)	D.Lgs. 10 marzo 2023, n. 24
Tipologia del trattamento	Raccolta e gestione delle segnalazioni
Categoria di interessati	Dipendenti, consulenti e collaboratori, con qualsiasi tipologia di contratto o incarico e a qualsiasi titolo, soci o persone con funzioni di amministrazione, vigilanza o rappresentanza, altri soggetti terzi che interagiscano con l'Ente, compresi i fornitori, consulenti, intermediari, ecc., nonché stagisti o lavoratori in prova, candidati a rapporti di lavoro ed ex dipendenti Facilitatori nella compilazione della segnalazione. Persone coinvolte nell'accertamento dei fatti segnalati. Utenti della piattaforma telematica.
Categoria di dati personali	Dati identificativi comuni relativamente agli utilizzatori della piattaforma informatica, al segnalante e a eventuali facilitatori. Le segnalazioni possono contenere dati di qualsiasi natura, anche particolari e/o relativi a condanne penali e reati.
Destinatari (categorie)	Incaricati e responsabili del trattamento elencati qui sotto.
Incaricati e Responsabili esterni del trattamento	In fase di gestione della segnalazione, i dati personali possono essere trattati da figure interne specificatamente autorizzate per le finalità indicate, nonché a fornitori di servizi o altri soggetti esterni (es. gestori di piattaforme impiegate per la gestione delle segnalazioni), che tratteranno i dati in qualità di responsabili del trattamento per conto dell'Azienda. Sussistendone gli estremi, i dati personali possono essere trasmessi a soggetti terzi a cui la comunicazione sia prevista per legge (ad es. Autorità Giudiziaria, Autorità nazionale anticorruzione, ecc.). In nessun caso i dati personali saranno oggetto di diffusione
Paese di destinazione	Italia
Paese di provenienza	Italia
Tempi di conservazione dei dati	5 anni.

Software utilizzato	Portale Telematico
Luogo di conservazione dei dati	
Trattamento cartaceo	
Luogo di conservazione degli archivi	
Rischi specifici sui dati	Alto rischio, per la tipologia del trattamento
Misure di sicurezza	M1 – M2 – M6 L'applicazione delle misure di sicurezza indicate consente di considerare il rischio residuo come accettabile
Scheda creata il	16.12.2023
Ultimo aggiornamento il	**16.12.2023**

LEGENDA DELLE MISURE DI SICUREZZA ORGANIZZATIVE, FISICHE, LOGISTICHE, PROCEDURALI PER LA MITIGAZIONE DEL RISCHIO

M1 – Formazione dei dipendenti incaricati del trattamento dei dati

La Società ritiene che sia necessario effettuare, con periodicità, una specifica formazione dei dipendenti in merito al corretto trattamento dei dati personali comuni e di contatto. In primo luogo la formazione riguarda i soggetti apicali, per gli aspetti organizzativi e giuridici del GDPR. Poi, più specificatamente, l'evento formativo viene calato nelle attività pratiche di gestione dei dati di ciascuno. Per tale adempimento ci si rivolge anche a consulenti esterni qualificati che conoscono, in modo approfondito, l'ambito lavorativo della Società e che sono dunque in grado di aiutare i dipendenti ad affrontare in modo corretto la normativa e a prevenire il rischio di trattamento non lecito di dati personali comuni e di contatto. La formazione comprende anche l'approfondimento sul Regolamento sull'uso degli Strumenti Informatici trattato nella misura M2.

M2 – Regolamento sull'uso degli strumenti informatici

E' uno specifico regolamento interno che disciplina l'utilizzo di strumenti informatici quali PC, notebook, smartphone, stampanti e loro relativi account nel contesto lavorativo. Tale misura si pone l'obiettivo di formare i dipendenti nel corretto uso degli strumenti, fatto che diminuisce il rischio di intrusione nei sistemi informativi della Società ed altresì di evitare il furto, l'accesso non autorizzato o distruzione di dati. Con l'occasione vengono altresì ribaditi i tempi di conservazione dei dati di accesso dei dipendenti agli Strumenti della Società e le modalità di verifica da parte del Titolare, anche alla luce dell'art. 4 comma 3 della L. 300/70 sul controllo degli strumenti di lavoro dei dipendenti.

M3 – Suddivisione per Unità/Aree di trattamento

La Società ha suddiviso la propria struttura in Unità/Aree di trattamento, all'interno delle quali sono inseriti i dipendenti sulla base dei compiti svolti. La suddivisione fa sì che il dipendente sia autorizzato a trattare solamente i dati personali comuni e di contatto indispensabili per poter svolgere le proprie mansioni, allineandosi così al cd principio di "minimizzazione dei dati" espresso dall'art 5 del Reg. 679/16. Per ciascuna area è individuato l'ambito di trattamento consentito, con apposito atto facente parte del Modello Organizzativo Privacy della Società. La documentata preposizione di un dipendente a tale area costituisce nomina ad incaricato. Secondo i principi di privacy by design, il sistema informativo della Società e i profili di autorizzazione ai gestionali, sono limitati agli ambiti individuati nelle Aree.

M4 – Rilascio informativa su singolo data entry

La Società rilascia idonea informativa ai sensi dell'art 13 del Reg. 679/16 per ogni canale di entrata di dati personali comuni e di contatto, per ciascuna attività di trattamento. Anche tramite rimando alla specifica pagina del sito web della Società.

M5 – Modulistica e processi volti a favorire l'esercizio diritti interessati

E' presenta una sezione privacy del sito della Società dove sono illustrati i diritti degli interessati ed è presente la modulistica per l'esercizio dei diritti. Gli interessati possono esercitare i diritti previsti dal Regolamento europeo in materia di protezione dei dati personali comuni e di contatto (GDPR) con le modalità specificate nell'informativa resa in sede di acquisizione dei dati personali comuni e di contatto. Tale informativa è altresì disponibile sul sito internet della Società nella sezione privacy. La misura prevede la realizzazione di una modulistica specifica messa a disposizione sul sito web.

M6 – Misure informatiche di prevenzione

Gli endpoint (computer, portatili, tablet) che accedono alla rete aziendale hanno installato un antivirus aggiornato. Sono inserite policy di limitazione di permessi, sia a livello di sistema operativo e sia di applicazione. La rete locale è presidiata da firewall monitorato. La posta elettronica usa protocollo cifrato.

Sono impostati e verificati i backup dei dati. Gli accessi remoti avvengono attraverso VPN.

M7 – Misure logistiche di prevenzione (distanze di cortesia, aree dedicate, ecc.)

Dove fisicamente possibile, la Società implementa all'interno della propria struttura idonee misure atte a preservare la riservatezza degli utenti e dei dati trattati. Per tale ragione sono previsti spazi d'attesa e aree per colloqui riservati.

M8 – Archivi cartacei

La Società predispone idonee misure per prevenire i rischi di accesso non autorizzato o non consentito agli archivi cartacei. Essi sono disposti in zone non accessibili al pubblico ovvero in zone in cui l'accesso è controllato. Tali archivi sono dotati di serratura, quando contenenti dati particolari o relativi a condanne penali e reati.